US006125447A

United States Patent [19]

Gong

[54] **PROTECTION DOMAINS TO PROVIDE SECURITY IN A COMPUTER SYSTEM**

[75] Inventor: **Li Gong**, Menlo Park, Calif.

[73] Assignee: **Sun Microsystems, Inc.**, Mountain View, Calif.

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,311,591	5/1994	Fischer	380/4
5,720,033	2/1998	Deo	713/200
5,758,153	5/1998	Atsatt et al.	395/614
5,841,870	11/1998	Fieres et al.	380/25
5,845,129	12/1998	Wendorf et al.	395/726
5,892,904	4/1999	Atkinson et al.	713/201

FOREIGN PATENT DOCUMENTS

2259590A	3/1993	WIPO	G06F 9/44
2308688A	7/1997	WIPO	G06F 12/14

OTHER PUBLICATIONS

Gong Li, et al.: "Going Beyond the Sandbox: An Overview of the New Security Architecture in the Java™ Development Kit 1.2", Proceedings of the Usenix Symposium on Internet Technologies and Systems, Monterey, CA, USA, 8–11 Dec. 1997, ISBN 1–880446–91–S, 1997, Berkeley, CA, USA, Usenix Assoc., USA, pp. 103–112, XP002100907.

Wallach, D. S., et al.: "Extensible Security Architectures for Java", 16th ACM Symposium on Operating Systems Principles, Sain Malo, France, 5–8 Oct. 1997, ISSN 0163–5980, Operating Systems Review, Dec. 1997, ACM, USA, pp. 116–128, XP–002101681.

Dean, D., et al., "Java Security: From HotJava to Netscape and Beyond," Proceedings of the 1996 IEEE Symposium on Security and Privacy, Oakland, CA, May 6–8, 1996.

Hamilton, M.A., "Java and the Shift to Net–Centric Computing," Computer, vol. 29, No. 8, Aug., 1996.

[57] **ABSTRACT**

A method and apparatus are provided for maintaining and enforcing security rules using protection domains. As new code arrives at a computer, a determination is assigned to a protection domain based on the source from which the code is received. The protection domain establishes the permissions that apply to the code. In embodiments where the code to be executed by the computer belongs to object classes, an association is established between the protection domains and the classes of objects. When an object requests an action, a determination is made as to whether the action is permitted based on the class to which the object belongs and the association between classes and protection domains.

24 Claims, 6 Drawing Sheets